NONLINEAR RANDOM SERIES GENERATOR

Publication number: JP63294115
Publication date: 1988-11-30
Inventor: RIN NAN RII; FUARUHADO HEMATEI
Applicant: COMMUNICATIONS SATELLITE CORP
Classification:
- international: ***G06F7/58; H03K3/84; H04L9/22; H04L9/26;*** **G06F7/58; H03K3/00; H04L9/18;** (IPC1-7): G06F7/58; H03K3/84; H04L9/04
- European: H03K3/84
Application number: JP19880112705 19880511
Priority number(s): US19870048697 19870512

Also published as:
EP0291405 (A2
US4852023 (A1
MX166449 (A)
EP0291405 (A3
EP0291405 (B1
more >>

Abstract not available for JP63294115
Abstract of corresponding document: **EP0291405**
Linear and nonlinear bits are logically combined to form each of at least three sequences, one of which i selectively used to couple either one of the others to the output of the sequence generator.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-139954
(43)Date of publication of application : 29.05.1990

(51)Int.Cl. H01L 23/50

(21)Application number : 63-294115
(22)Date of filing : 21.11.1988

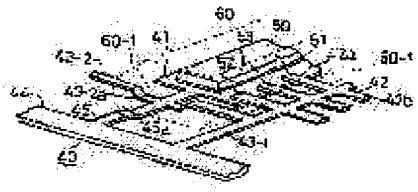
(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : OOUCHI NOBUHITO

(54) LEAD FRAME AND RESIN-SEALED SEMICONDUCTOR DEVICE USING SAME

(57)Abstract:

PURPOSE: To perform bonding easily with accuracy by the use of a wire between a semiconductor element and each inner end part of a lead by causing a stepped part to be formed outside the region for sealing of a suspended lead with resin so that an element loading part is located at a position lower than the inner end part.

CONSTITUTION: A plurality ot leads 42 are disposed near an element loading part 41 of a lead frame 40 and each lead has inner and outer end parts 42a and 42b and respective leads 42 are coupled and supported by a tiebar 43-1 which is fixed to a frame part 44. As the element loading part 41 is spaced at a prescribed interval (h) 2 from the inner end part 42a and is located at a position lower than the above inner end part, a stepped part 45a is formed at a suspended lead 45 that is outside the region of resin-sealing and accordingly, the stepped part 43-2a is formed even at a tiebar 43-2. Since the stepped part 45a of the suspended lead 45 is formed outside the region of resin-sealing, such a large stepped part 45a is formed in this way and its formation of the stepped part makes it possible to prevent an edge short circuit which takes place between a wire 53 and a semiconductor element 50 and further, it makes the wire 53 longer. Connection work is thus performed easily with accuracy.



⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63-294115

⑤Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和63年(1988)11月30日
H 03 K 3/84		8626-5J	
G 06 F 7/58		7056-5B	
H 04 L 9/04		7240-5K	審査請求　未請求　請求項の数 16　(全6頁)

⑭発明の名称　非線形ランダム系列発生器

⑳特　願　昭63-112705

㉒出　願　昭63(1988)5月11日

優先権主張　㉜1987年5月12日㉝米国(US)㉞048697

⑰発明者　リン　ナン　リー　アメリカ合衆国、メリーランド州、ポトマック、フォンテイン　ストリート　7605

⑰発明者　ファルハド　ヘマティ　アメリカ合衆国、メリーランド州、ジャーマンタウン、フレデリック　ロード　19405

⑪出願人　コミュニケーションズ　サテライト　コーポレーション　アメリカ合衆国、ワシントン　ディーシー、エスダブリュー、ランファン　プラザ　950

⑭代理人　弁理士　石川　泰男　外2名

明　細　書

1．発明の名称

非線形ランダム系列発生器

2．特許請求の範囲

1．非線形系列出力を発生させる非線形系列発生器において、

第1の系列を発生させる第1の発生手段(130)と、

第2の系列を発生させる第2の発生手段(132)と、

第3の系列を発生させる第3の発生手段(136)と、

第4の系列を発生させる第4の発生手段(140)と、

第5の系列を発生させる第5の発生手段(138)と、

第6の系列を発生させる第6の発生手段(142)と、

前記第1及び第2の系列を結合して第1の結合系列を得るようにする第1の結合手段(134)と、

前記第3及び第4の系列を結合した第2の結合系列を得るようにする第2の結合手段(144)と、

前記第5及び第6の系列を結合して第3の結合系列を得るようにする第3の結合手段(148)と、及び

前記第2の結合系列に従って、前記第1及び第3の結合系列のうちの1つの結合系列を前記出力非線形系列として選択的に通過させる出力手段(120,122,124,126)と、を含むことを特徴とする非線形ランダム系列発生器。

2．請求項1記載の非線形系列発生器において、前記第1～第6の系列のそれぞれは、ほぼランダムである非線形ランダム系列発生器。

3．請求項1記載の非線形系列発生器において、前記第1、第3、及び第5の系列は、線形系列であり、系列の各ビットが該系列の以前のビットの線形関数であるようになっている非線形系列発生器。

4．請求項3記載の非線形系列発生器において、前記第2、第4、及び第6の系列は、非線形系列であり、該非線形系列の1つの系列の各ビットが前記線形系列の1つの系列の以前のビットの非線形関数であるようになっている非線形系列発生器。

5．請求項4記載の非線形系列発生器において、前記第2の系列の各ビットは、前記第1の系列で以前に発生させられたビットの非線形関数である非線形系列発生器。

6．請求項5記載の非線形系列発生器において、前記第4の系列の各ビットは、前記第3の系列で以前に発生させられたビットの非線形関数である非線形系列発生器。

7．請求項6記載の非線形系列発生器において、前記第6の系列の各ビットは、前記第5の系列で以前に発生させられたビットの非線形関数である非線形系列発生器。

8．請求項4記載の非線形系列発生器において、前記第6の系列の各ビットは、前記第1の系

列で以前発生させられビットの非線形関数である非線形系列発生器。

9．請求項8記載の非線形系列発生器において、前記第2の系列の各ビットは、前記第5の系列で以前に発生させられたビットの非線形関数である非線形系列発生器。

10．請求項1記載の非線形系列発生器において、前記第1～第3の結合手段は、モジュロ・2加算器を含む非線形系列発生器。

11．請求項1記載の非線形系列発生器において、前記出力手段は、

前記第1及び第2の結合手段を結合して第4の結合系列を得るようにする第4の結合手段(120)と、

前記第2及び第3の結合系列を結合して第5の結合系列を得るようにする第5の結合手段(122, 124)と、

前記第4及び第5の結合系列を結合して前記非線形系列出力を得るようにする第6の結合手段(126)と、を含む非線形系列発生器。

12．請求項11記載の非線形系列発生器において、前記第4及び第5の結合手段は、アンドゲートを含み、前記第5の結合手段は、前記第2の結合系列を受ける反転入力を有するようになっている非線形系列発生器。

13．請求項12記載の非線形系列発生器において、前記第6の結合手段は、モジュロ・2加算器を含む非線形系列発生器。

14．請求項1記載の非線形系列発生器において、前記第1、第3、及び第5の発生手段は、r，s，及びtをそれぞれ有する線形フィードバックシフトレジスタを含み、ここで、r，s，及びtは、異なる整数である非線形系列発生器。

15．請求項14記載の非線形系列発生器において2^r-1，2^s-1，及び2^t-1は、相対的に素数である非線形系列発生器。

16．出力非線形系列を発生させる非線形系列発生器であって、前記系列発生器は、第1予備系列を発生させる第1の手段(114)と、第2の予備系列の予備系列を発生させる第2の手段(118)

と、及び、前記第1及び第2の予備系列を結合して前記出力非線形系列を形成するようにする手段(116)と、を含む形式である非線形系列発生器において、

前記第1の手段は、第1の線形系列のビットであって各ビットが該第1の線形系列で以前に発生させられたビットの線形関数であるビットを発生させる第1の線形手段(130)と、第1の非線形系列のビットであって各ビットが該第1の線形系列で以前に発生させられたビットの非線形関数であるビットを発生させる第1の非線形手段(132)と、及び、前記第1の線形及び非線形系列を結合して前記第1の予備系列を得るようにする第1の結合手段(134)と、を含み、及び、

前記第2の手段は、第2の線形系列のビットであって各ビットが該第2の線形系列で以前に発生させられたビットの線形関数であるビットを発生させる第2の線形式手段(138)と、第2の非線形系列のビットであって各ビットが該第2の線形系列で以前に発生させられたビットの非線形関数で

あるビットを発生させる第２の非線形手段(142)と、及び、前記第２の線形及び非線形系列を結合して前記第２の予備系列を得るようにする第２の結合手段(146)と、を含むことを特徴とする非線形系列発生器。

３．発明の詳細な説明

〔産業上の利用分野〕

本発明は、通信の安全性の分野に関し、より詳細には、通信の安全性を維持するのに使用され得るランダム系列発生器(Random Sequence Generators)に関する。

〔従来の技術、発明が解決しようとする課題〕

通信の安全性が望まれるシステムにおいて、伝達されるべきデータを暗号化したりあるいは混乱させる(scramble)ことは一般的であるが、得られる安全性の程度は、権限ない使用者が使われている暗号キーあるいは混乱系列を決定するのに直過する困難性の程度に依存する。それゆえ、安全な通信にとって、暗号キーあるいは混乱(scramble)

系列が高程度のランダム性を有することが緊急である。

従来の定義によれば、２値系列が、エス ダブル ゴロム(S.W.Golomb)による『シフト レジスタ シーケンス』、ホルドン デイ(Holden Dey)、サンフランシスコ、１９６７年に示されるような“ランダム性の公理”を満足するならば、ランダムな（ランダムにみえる）系列である。ランダム性の公理を満足する系列が安全性システムの運用にとって必ずしも適切でないことは周知である。良いランダム系列について他の望ましい特性は、系列の複雑性（いくつかの基準に従って定義される）、及び“転換可能性(invertibilty)に関連する問題、すなわち、フィードバック関数が既知であると仮定して出力系列のブロックから“種(seed)”を見つけるに必要とされる計算の複雑性を含む。

それゆえ、多くの安全通信システムの本質的部分は、ランダム系列発生器である。ランダム系列の発生のいくつかの技術が知られており、最も簡

単な技術は、線形あるいは非線形のフィードバック回路を有するシフトレジスタの使用を伴っている。非線形フィードバックシフトレジスタは、安全通信にとって、より適用でき魅力的である。

所定のm段シフトレジスタにとって、約$2^{2^{m-1}-m}$個の非線形フィードバック回路は、発生させられる系列が従来のランダム性の公理を満足するように、存在する。現在のところ、合理的な複雑性でフィードバック関数を設計する一般的な構成技術は、知られていない。非線形系列を構成するための多くの解析方法は、線形系列の連鎖に基づいているが、安全の目的のためにこのような系列を使用するのは、安全ではない。

非線形系列を発生する一般的な方法は、第１図に示されるように、線形ＰＮ系列に基づく非線形関数を適用することである。これは、一般に、グロス(Groth)発生器として知られている。第１図において、線形フィードバックシフトレジスタ（ＬＦＳＲ）１０は、線形ＰＮ系列を発生させ、そして、非線形関数発生器は、１２で概略的に示

されている。この技術の主な欠点は、非線形関数の任意の選択が一般に所望のランダム特性を有する系列の発生にならないということである。更に、いくつかの特定の場合を除いて、例えば、イー エル キー(E.L.Key)、“非線形２値系列発生器の構成及び複雑性の解析”、アイイーイーイー トランザクションズ オン インフォメーション セオリー(IEEE Transactions on Information Theory)、１１月１９７６年に述べられているような場合を除いて、発生される系列の複雑性は、解析されていない。

非線形系列を発生させる他のものは、ゲッフェ(Geffe)により設計され、イー エル キーによる上記の引用文献で述べられている系列発生器である。第２図に示されているゲッフェの発生器は、３つの線形フィードバックシフトレジスタ１４，１６，及び１８と、アンドゲート２０と、１つの反転入力２４を有するアンドゲート２２と、及びモジュロ－２加算器（排他的論理和ゲート）２６と、から構成されている。この構成において、線

形フィードバックシフトレジスタ１６は、制御レジスタとして使用され、線形フィードバックシフトレジスタ１４あるいは１８のいずれか一方から（両方ではない）の系列を排他的論理和ゲート２６を介して出力に選択的に接続するようにする。制御レジスタ１６からの現在の出力が論理１であるならば、線形フィードバックシフトレジスタ１４からの出力は、排他的論理和ゲート２６に接続され、そして、系列発生器の出力に接続される。そうでない場合には、線形フィードバックシフトレジスタ１８からの出力は、系列発生器の出力になる。

同じ系列を正確に発生するであろう線形フィードバックシフトレジスタの段の数に関して、第２図の系列発生器の複雑性は、ｒｓ＋（ｓ＋１）ｔに等しく、ここで、ｒ，ｓ，及びｔは、それぞれ線形フィードバックシフトレジスタ１４，１６及び１８の原特性多項式の次数である。出力系列の周期は、2^r-1，2^s-1及び2^t-1の最小公倍数である。

出力で０及び１をバランスよく配分することは、第２図の発生器の主な利点である。しかしながら、含まれる線形項のために、出力系列から“番”を見つけることは、むしろ容易である。第２図の発生器（ゲッフェの発生器）の複雑性は、グロスの発生器を成分レジスタとして使用することにより、増加させられ得る。

イー　エル　キー、及び、イー　アイ　グロス、“制御可能な複雑性を有する２値系列の発生”アイイーイーイー　トランザクションズ　オン　インフォメーション　テオリー、(IEEE Transactions on Information Theory)１９７１年５月の上記の引用文献を参照。しかしながら、この場合に、所望のランダム特性は、保証されない。

従って、本発明の目的は、適切な複雑性及びランダム性をもつ系列を発生させるランダム系列発生器を提供することにある。

〔課題を解決するための手段、作用〕

上記課題を解決するために、本発明は非線形系列出力を発生させる非線形系列発生器において、

第１の系列を発生させる第１の発生手段と、第２の系列を発生させる第２の発生手段と、第３の系列を発生させる第３の発生手段と、第４の系列を発生させる第４の発生手段と、第５の系列を発生させる第５の発生手段と、第６の系列を発生させる第６の発生手段と、前記第１及び第２の系列を結合して第１の結合系列を得るようにする第１の結合手段と、前記第３及び第４の系列を結合した第２の結合系列を得るようにする第２の結合手段と、前記第５及び第６の系列を結合して第３の結合系列を得るようにする第３の結合手段と、及び前記第２の結合系列に従って、前記第１及び第３の結合系列のうちの１つの結合系列を前記出力非線形系列として選択的に通過させる出力手段と、を含んで構成されたことを特徴とする。

要約すると、本発明は、少なくとも第１及び第２の系列が制御系列により系列発生器の出力に選択的にゲートされる点においてゲッフェの発生器の構成とほぼ同様の構成を利用することにより、複雑性およびランダム性の有利な組合せを達成する。しかしながら、本発明の好適な実施例において、第１、第２、及び制御系列は、線形系列及び非線形系列の結合から生じる。

〔実施例〕

以下、本発明の第１実施例について、第３図を参照して述べる。

第２図と第３図との比較からわかるように、第３図は、３つの非線形系列の発生において、本質的に同様であり、第２系列は、制御系列として使用され、第１及び第３系列のいずれか一方を系列発生器の出力に選択的にゲートさせている。それゆえ、ゲート１２０，１２２，及び１２６，及びインバータ１２４の機能は、それぞれ、第２図の対応する部分２０，２２，２６，及び２４の機能と本質的に同じである。第３図に示される本発明の第１の実施例における本質的な相違は、系列発生器の手段それら自身にある。第２図の簡単な線形フィードバックシフトレジスタ１４の代わりに、第３図の実施例は、線形フィードバックシフトレジスタ１３０から系列発生器１１４を形成し、こ

れは、ブロック１３２で概略的に示される非線形関数を含む。“種”、すなわち、線形フィードバックシフトレジスタ１３０の初期状態は、０及び１のどんな非０のブロックであってもよい。各時間間隔で、系列発生器１１４は、１つの線形ビット及び１つの非線形ビットを発生させ、線形ビットは、以前に発生させられたビットの線形関数によってつくられ、一方、非線形ビットは、以前に発生させられた線形ビットの非線形関数である。線形及び非線形ビットは、それから、モジュロ－２加算器１３４で結合される。第２及び第３系列発生器１１６及び１１８は、同様に、それぞれ、非線形関数１４０及び１４２を有する線形フィードバックシフトレジスタ１３６及び１３８から構成され、線形及び非線形は、アンドゲート１４４及び１４６で結合される。

第３図の線形フィードバックシフトレジスタ１３０，１３６，及び１３８は、クロックにより調整され、それぞれ、どんな数の段ｒ，ｓ，及びｔをも含み得る。長いサイクルを構成するために、

2^r-1，2^s-1，及び2^t-1がそれぞれ素数である。すなわち、それらが公因数を有しないように、ｒ，ｓ，及びｔが選択されることが好ましい。非線形関数ＮＬ１，ＮＬ２，及びＮＬ３は、グロス発生器、あるいは、０及び１の合理的なバランスをもついかなる他の関数によっても、選択され得る。

第３図の実施例は、０及び１の合理的なバランスをもつ非線形系列を発生させる。しかしながら、第３図の構成の線形項のために、システムが暗号解読の攻撃をいくらか受け易いことが示され、すなわち、出力系列のブロックから“種”を見つけるのは、可能かもしれない。この課題を解決するために、本発明の第２実施例を第４図に示す。第２の系列発生器２１６からの線形及び非線形ビットは、第３図の系列発生器１１６からの線形及び非線形ビットが加算されのと同じ方法で、モジュロ－２の加算が行われる。しかしながら、第４図の構成においては、第１のシフトレジスタ２３０

からの線形ビットは、第３の系列発生器の非線形ビットと結合され、一方、第１の系列発生器の非線形ビットは、第３の系列発生器の線形ビットに加算される。これは、いかなる所定の結合系列内の線形ビットも該系列の非線形ビットに関連しないので、複雑性を向上させる。

〔発明の効果〕

本発明により達成される系列発生器によれば、出力系列のブロックから“種”を見つけるのに必要な計算の複雑性が向上する。大規模なシミュレーションテストは、発生される系列が０及び１の良いバランスを有し、そして、その実行された長さの配分(its run length distribution)が理想状態に驚くほど近いことを示した。

４．図面の簡単な説明

第１図は線形フィードバックシフトレジスタの中に非線形関数を適用する従来の系列発生器のブロック図、

第２図は従来技術において知られている他の非線形系列発生器のブロック図、

第３図は本発明の第１実施例による系列発生器のブロック図、

第４図は本発明の第２実施例よる系列発生器のブロック図である。

１１４，１１６，１１８…系列発生器、
１２０，１２２，１２６…ゲート、
１２４…インバータ、
１３０，１３６，１３８…線形フィードバックシフトレジスタ
１３２，１４０，１４２…非線形関数、
１３４，１４４，１４６…２を法とする加算器
２１４，２１６，２１８…系列発生器。

出願人代理人　石　川　泰　男

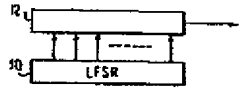


FIG.1

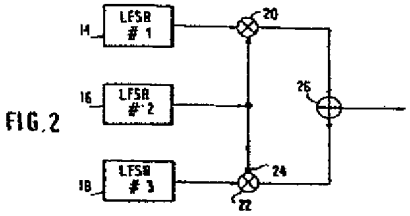


FIG.2

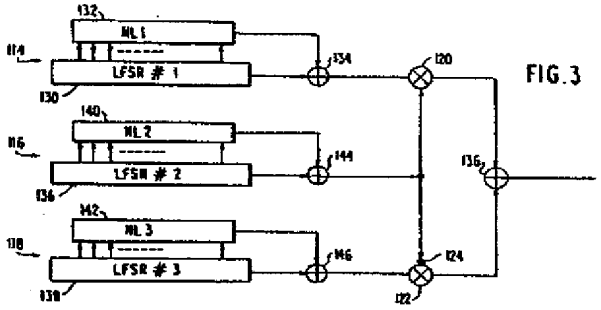


FIG.3

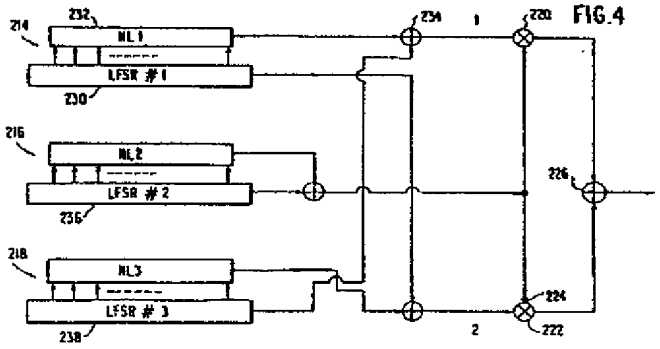


FIG.4